Blockchain Technology & Intellectual Property Protection

Yiyao Wu, Dillon Ambersley, Ava Filipour, Suma Bindu
Advisor Dr. Omar Abuzaghleh
Department of Computer Science and Computer Engineering
University of Bridgeport, Bridgeport, CT

Abstract

In Year 2008, Satoshi Nakamoto titled *Bitcoin: A Peer-to-Peer Electronic Cash System* , which made the whole world stunning and enabled people starting to concentrate on Bitcoin and the technology behind it. Even though Bitcoin is an extrodinary world famous intelegence contribution on 21st Century, it's still a tip of the iceburg to the technology behind it — Blockchain Technology.

In this poster, we give more space on explaining the working principle of Blockchain Technology and also take a quick glance at the application of Blockchain Technology in Intellectual Property Protection field.

Introduction

As the whole world move their attention to Bitcoin, more and more people start studying the 'magic' behind it. The real mystic power — Blockchain Technology.
Blockchain technology has been developed for many years but until 2008, the birth of Bitcoin brought this technology into the public sight. Whatever Bitcoin or Blockchain, they are all used to transfer information by encryption. They could be applied in fianace, public safety, education, medicine and other potential domains.

Background

The first work on a cryptographically secured chain of blocks was described in 1991 by Stuart Haber and W. Scott Stornetta. But the first blockchain was conceptualized by a person (or group of people) known as Satoshi Nakamoto in 2008.

Within this year, in United States, the famous 2008 Financial Crisis broke out. The public lost their trust on the existed finance system,which cause people starting to look for a way out from other fields. Based on this situation, Satoshi Nakamoto proposed the conception of Electric Currency — Bitcoin. But what is Bitcoin exactly?

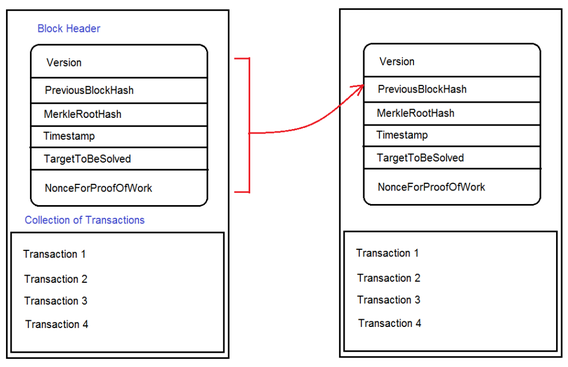
The Nature of Blockchain

Essentially, Bitcoin is a Blockchain based successful trial or product. Because the most obvious characters of Bitcoin are Nonrenewability (Bitcoin Issuance is limited) and Slow Trading Speed. That's destined Bitcoin can not replace current currency system. But why we still think Bitcoin is a milestone of Blockchain developement? Thus,we have to know what is Blockchain at first.

Definition: *Blockchain is a distributed database of records, which is secure, public,decentralized and permissionless.* Because of Blockchain using cryptographic hash (a very complicated algorithm) to record data and being allocated to the whole blockchain network, it's almost impossible to manage and modify.

Consists of Blockchain

The basic unit of Blockchain is a Block. Each block contains two parts: Header and Body. Block body is related to the header and used to store data information. Block header is generated by hash and used to store lots of feature values, such as previous block hash, current block hash, Timestamp, Transaction data and etc.. The hash value is a unique 256 bit binary number. Only the value, which can match all the conditions of previous block, can be finally thought as valid, that is, only one block can be connected to the chain at each time.



Hash & Blockchain

As mentioned before, block header is generated by hash. But what is hash? 'Hash' means computer can calculate a feature value of the same length for any content. The hash length of the blockchain is 256 bits, which means that no matter what the original content is, a 256-bit binary number is finally calculated. The 256-bit binary number is corresponding to the hash and also, the hash must be changed as long as the original content is changed. Therefore, we have two corollaries as below:

Corollary 1: The hash of each block is different, and the block can be identified by hashing.

Corollary 2: If the content of the block changes, its hash must change.

The Immunability of Hash

The block and the hash are in one-to-one correspondence, and the hash of each block is calculated to generate the 'Header'. Computer can use the feature value which is contained in Header to generate a long string. Hash value is calculated from this string. Here's the formula of Hash:

$$\text{Hash} = \text{SHA256 (block header)}$$

Above is the calculating formula of hash. SHA256 is the hash algorithm of the blockchain. Noticed that, this formula contains only the block header but does not contain the block body. That is, the hash is uniquely determined by the block header.

As mentioned earlier, the block header contains a lot of content, including the hash of the current block, and the hash of the previous block. This means if the contents of the current block are changed, or if the hash of the previous block is changed, the content (Blockbody) must be changed.

Mining and Difficulty Coefficient

Mining is a vivid metaphor of recording valid ledgers to a computer. Because the essence of Blockchain is a decentralized ledger, each user is on the peer level. So why we have to store other users' ledgers in our computers? The basic reason is a blockchain need a steady stream of blocks to extend its length. But the system can not generate new blocks by itself. Thus, the blockchain system need to 'hire' some users to help generate new blocks. Correspondingly, these users (we called them Miners) can earn some benefits (such as Bitcoin). This progress help every user synchronize their information to the whole network. In detail, every miner should do a massive of calculations to find a uniquely valid 'Hash' value. Because this progress can be seen as to find a matched sand from desert, so people assimilate it to mining.

Difficulty Coefficient. As mentioned, blockchain is decentralized. How can we test the reliability of each block. The principle is that the longest chain is authentic. But a long chain means more blocks and more blocks means more calculations. Thus, only the people (or group of people) who can master 51% more calculating capability is authentic. But practically, people can not compete against the whole network individually. Therefore, the longest chain represents this record is tested by most blockchain users, that is, the longest chain is real. To ensure the real records can be kept and extended, Satoshi Nakamoto proposed adding difficulty coefficient in the progress. The basical principle of hashing is to find a small value, called target, which is less than the maximum target value. If the target is less than targetmax, then think this value is valid, otherwise, the computer has to recalculate it until the correct value is found out. Thus, people can gurantee the record's reliability by this way.

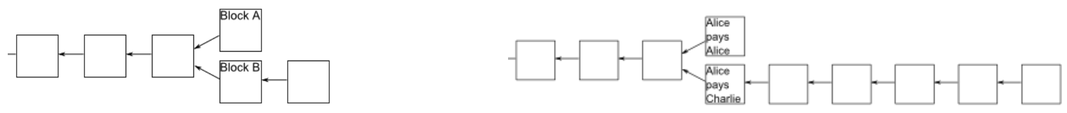
```
target = targetmax / difficulty
```

```
targetmax = 0x00000000FFFF0000000000000000000000000000000000000000000000000000
difficulty = 14484.162361
```

Hard Fork in Blockchain

Even if the blockchain is reliable, there is still a problem not solved: if two people write data to the blockchain at the same time, which block should we follow?

The solution is the new node always uses the longest blockchain. If the blockchain has a fork, we only follow the chain which can reach 6 blocks first (called "six confirmations").



Blockchain Technology in IP Protection

IP Protection By Law:
1.Prove Ownership. Only Registered Patent can be protected.
2.Only when your patent is stolen and used for commercial reason, your rights can be defended.
3.Higher expense on Law suite and hiring lawyer.
4.The progress of taking evidence is long and difficult.

Protect IP by Blockchain Technology
If we use blockchain technology to protect our Intellectual Properties, the situation will be different. Combining the features of Blockchain as mentioned before (immunability, security, openess and etc.), we can protect our IP in an efficient and smart way.

1. Upload your work on Blockchain Network and generate your own secret key (a hash value which contains owner, timestamp, transaction relationship, trade expense, content).
2. The people(or group) who pay for using your work can only aquire unique secret key from your block.
3.After the user complete using your work, the new status information and new timestamps will be recorded down to the next block.

All these progress are synchronized to the whole blockchain network after every action is completed. Since the work owner's individual electronic signature is written into the original block, nobody can change the information, only if change it from the initial block. But it's almost impossible to achieve, because only the owner has the initial secret key. If a hacker modified the data of the blockheader, the whole block will be changed. If your personal chain is under attacked and destroyed, you can still restore it by copying the data from the blockchain network (if you complete synchronizing). Thus, blockchain technology can efficiently protect your intellectual properties.

Conclusion

The blockchain, as an unmanaged distributed database, has been operated for 11 years since 2009, without major problems. This proved the Blockchain technology is feasible.

However, in order to ensure the reliability of the data, the blockchain also has its own cost.
1. Efficiency. Data need to be written into the blockchain and wait for at least ten minutes to ensure all nodes can be completely synchronized. it takes more time.
2. Energy consumption. Block generation requires mining machines to execute countless meaningless calculations to find the only unique correct Hash value. This progress consumes a lot of energy.

Therefore, the executable scenario of the blockchain is actually very limited.

1. **There is no authorities that all members trust.**
2. **The recorded data is not required to be used frequently.**
3. **The benefits from mining can balance its cost.**

If the above conditions are not met, the traditional database is a better solution.